



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/874,574	06/04/2001	Robert David Graham	03845P003	5484

7590 11/29/2005

W. Scott Petty
KING & SPALDING
191 Peachtree Street
45th Floor
Atlanta, GA 30303-1763

EXAMINER

NALVEN, ANDREW L

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 11/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/874,574	Applicant(s) GRAHAM, ROBERT DAVID	
	Examiner Andrew L. Nalven	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 13 September 2005.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,3,4,6-14,16-40,42-50 and 52-57 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,3,4,6-14,16-40,42-50 and 52-57 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 04 June 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1, 3-4, 6-14, 16-40, 42-50, and 52-57 are pending.
2. Amendment submitted 13 September 2005 has been entered and considered.

Response to Arguments

3. Applicant's arguments with respect to claims 1, 3-4, 6-14, 16-40, 42-50, and 52-57 have been considered but are not persuasive.
4. Applicant has argued on pages 18-20 that the Gleichauf and Vaidya references fails to teach a table that comprises contextual information, data signatures, and alert condition values. Examiner has provided a new reference, Olden US Patent No. 6,460,141 to provide teachings for the use of tables for storing information related to network intrusion attacks (Olden, column 27 lines 25-33). Examiner respectfully disagrees that the Gleichauf and Vaidya fail to teach the storing of contextual information, data signatures, and alert condition values. Gleichauf teaches the storing of an attack signature list (Gleichauf, column 9 lines 32-37) that includes alert condition values (Gleichauf, Figure 5B, low med high) and data signatures (Gleichauf, column 6 lines 40-45). Given its broadest reasonable interpretation, contextual information is also taught being stored by Gleichauf through his teaching of storing traffic signatures of known policy violations. Contextual information refers to the context of a data communication. Gleichauf's data signature contains the context of the data. Thus,

Art Unit: 2134

Gleichauf teaches contextual information. Given a more narrow interpretation, such as the interpretation offered by Applicant on page 18 of the arguments submitted 13 September 2005 (notes contextual data can comprise at least one of an application layer data field type or an application layer protocol type), Vaidya provides teachings which meet the limitation. Vaidya teaches the monitoring of application layer communications (column 10 lines 16-21) using attack signatures which include protocol header field information (Vaidya, column 10 lines 25-45, header field). Thus, Gleichauf and Vaidya teach the use of contextual information, data signatures, and alert condition values and the combination of Gleichauf, Vaidya, and Olden provide all of the claimed limitations.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1, 3-4, 6, 14, 18-21, 25-26, 32, 34, 37-40, 42, 50, and 54-56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al US Patent No. 6,301,668 in view of Vaidya US Patent No. 6,279,113 and Olden US Patent No. 6,460,141.

7. With regards to claims 1, 14, 18, 37, 50, 54, 56, Gleichauf teaches the creating of a list of attack signatures comprising data signatures, and alert condition values (Gleichauf, Figure 5B, column 9 lines 32-37, column 6 lines 40-45), detecting of a data signature (Gleichauf, column 6 lines 36-45), the correlating of the data signature with a fingerprint of the target to determine to what extent the target is vulnerable to the data signature (Gleichauf, column 6 lines 51-56, likelihood of success), comparing the contextual information and the data signature to the group of attack signatures (Gleichauf, column 6 lines 36-40), and the assigning of an alert condition value to the data signature based on the comparison of the contextual information and data signature to data in the table (Gleichauf, column 8 lines 28-52, determined probability of success). Gleichauf fails to teach the detecting, correlating, and evaluating of data signatures at the application layer and the use of tables. Vaidya teaches the evaluating of communications at the application layer (Vaidya, column 10 lines 25-45, application layer, column 8 lines 1-24) and evaluating contextual information related to the data signature to determine a likelihood that said target is under attack, the contextual information comprising at least one of an application layer data field type used to encapsulate the data signature and an application layer protocol type used to transmit the data signature (Vaidya, column 10 lines 25-45, column 10 lines 16-21). Olden teaches the storing of attack data in tables (Olden, column 27 lines 25-33). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Vaidya's method of evaluating application layer communications and Olden's method of storing data in tables because they offer the advantage of greater

security by ensuring that attacks based on any of the OSI's seven layers may be detected and the assurance that sensitive files will be monitored to stop unlawful access (Vaidya, column 4 lines 29-39, column 1 lines 19-45) and provides a method of storing attack data with a simple way of adding and deleting potential attack data (Olden, column 27 lines 25-33).

8. With regards to claims 25, 34, 38, Gleichauf as modified teaches the evaluating of contextual information relating to the data signature to determine a likelihood that the target is under attack (Gleichauf, column 6 lines 25-36).

9. With regards to claims 3, 20, 39, Gleichauf as modified teaches the fingerprint including a target node's operating system (Gleichauf, column 3 lines 62-65).

10. With regards to claims 4, 21, 40, Gleichauf as modified teaches the fingerprint including the node's processor type (Gleichauf, column 3 lines 62-65, devices, column 7 lines 1-4).

11. With regards to claims 26, Gleichauf as modified teaches the contextual information including a particular network protocol with which the data signature was transmitted (Gleichauf, column 8 lines 28-45, column 6 lines 25-36).

12. With regards to claim 6, 42, Gleichauf as modified teaches the generating of a first alert condition upon determining that the target node is vulnerable to the data signature (Gleichauf, column 8 lines 28-52, determined probability of success, prioritizing monitoring).

13. With regards to claims 19, 55, Gleichauf as modified teaches the fingerprint including a particular service executed on the target (Gleichauf, column 7 lines 51-60, services).

14. With regards to claim 32, Gleichauf as modified teaches the profiling of the target to determine which ports are open by passively listening to what traffic succeeds in talking to/from the target (Gleichauf, column 7 lines 40-49).

15. Claims 7-8, 10-12, 22, 27, 29-31, 43-44, 46-48, 57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al US Patent No. 6,301,668, Vaidya US Patent No. 6,279,113, and Olden US Patent No. 6,460,141, as applied to claims 1, 18, 25, 37, 44, and 56 above, and in further view of Conklin et al US Patent No. 5,991,881. Conklin teaches a network surveillance system.

16. With regards to claims 7, 43, Gleichauf as modified fails to teach the listening for a response to a data signature from the target. Conklin teaches the listening for a response to a data signature from the target (Conklin, column 6 lines 21-43, column 7 lines 25-29, evidence logging function). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Conklin's method of listening with Gleichauf's adaptive security system because it offers the advantage of ensuring continuing reporting of all pertinent activities following the detection of a predefined alert condition (Conklin, column 1 lines 35-49).

17. With regards to claims 8, 44, Gleichauf as modified teaches the determining whether the target node's response or lack of a response is suspicious (Gleichauf, column 7 lines 29-38).

18. With regards to claims 10, 46, Gleichauf as modified teaches the generating of a second alert condition upon determining that the target node's response or lack of a response is suspicious (Conklin, column 7 lines 25-38, alert notification).

19. With regards to claims 11, 47, Gleichauf as modified teaches the combining of the second alert with the first, thereby updating the first alert with information within the second alert (Conklin, column 8 lines 6-14, column 7 lines 44-50).

20. With regards to claims 12, 48, Gleichauf as modified fails to teach the listening for behavior of the target node and sending an alert condition. Conklin teaches the listening for behavior of the target node (Conklin, column 8 lines 1-5) and generating a second alert condition upon determining that the target node's behavior is suspicious (Gleichauf, column 7 lines 51-61). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Conklin's method of listening to the behavior of the target with Gleichauf's adaptive security system because it offers the advantage of ensuring continuing reporting of all pertinent activities following the detection of a predefined alert condition (Conklin, column 1 lines 35-49).

21. With regards to claims 22, 29 and 57, Gleichauf as modified fails to teach the monitoring of responses from the target following the data signature and determining a likelihood of whether the target is under attack based on the data signatures of the responses. Conklin teaches the monitoring of responses from the target following the

Art Unit: 2134

data signature and determining a likelihood of whether the target is under attack based on the data signatures of the responses (Gleichauf, column 7 lines 29-38). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Conklin's method of listening with Gleichauf's adaptive security system because it offers the advantage of ensuring continuing reporting of all pertinent activities following the detection of a predefined alert condition (Conklin, column 1 lines 35-49).

22. With regards to claim 27, Gleichauf as modified fails to teach the protocol being FTP. Conklin teaches the protocol being FTP (Conklin, column 3 lines 8-14). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Conklin's method of monitoring FTP with Gleichauf's adaptive security system because it offers the advantage of allowing the monitoring of one of the principal network protocols used to transfer files.

23. With regards to claims 30-31, Gleichauf as modified fails to teach the current state comprising an inbound or outbound connection from the target following a detected signature. Conklin teaches the current state comprising an inbound or outbound connection from the target following a detected signature (Conklin, column 8 lines 1-5). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Conklin's method of listening with Gleichauf's adaptive security system because it offers the advantage of ensuring continuing reporting of all pertinent activities following the detection of a predefined alert condition (Conklin, column 1 lines 35-49).

Art Unit: 2134

24. Claims 9, 23 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al US Patent No. 6,301,668, Vaidya US Patent No. 6,279,113, Olden US Patent No. 6,460,141, and Conklin et al US Patent No. 5,991,881, as applied to claims 8, 22, and 44 above, and in further view of Krumel US PGPub 2002/0083331.

25. With regards to claims 9, 23 and 45, Gleichauf as modified above fail to teach the determining if a packet is an unknown command. Krumel teaches the determining if a packet is an unknown command (Krumel, Page 7, Paragraph 0085, unknown packet type). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Krumel's method of detecting unknown commands because it offers the advantage of ensuring that no packets that do not fit set security filters are allowed to pass in and out of a network (Krumel, Page 7, Paragraph 0085 and Page 7 Paragraph 0087).

26. Claims 13 and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al US Patent No. 6,301,668, Vaidya US Patent No. 6,279,113, Olden US Patent No. 6,460,141 and Conklin et al US Patent No. 5,991,881, as applied to claims 11 and 47 above, and in further view of Zhang et al "Detecting Backdoors."

27. With regards to claims 13 and 49, Gleichauf as modified above fails to teach suspicious behavior comprising the transmitting of a root shell prompt to a suspect node. Zhang teaches teach suspicious behavior comprising the transmitting of a root shell prompt to a suspect node (Zhang, Page 12, Section 4.5, Root Backdoor). At the time the invention was made, it would have been obvious to a person of ordinary skill in

the art to utilize Zhang's method of detecting root shell transmissions with Gleichauf as modified because it offers the advantage of preventing an attack from gaining unauthorized access to a system by the use of a backdoor (Zhang, Page 1 Section 1.Introduction).

28. Claims 16, 35, and 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al US Patent No. 6,301,668, Vaidya US Patent No. 6,279,113, and Olden US Patent No. 6,460,141, as applied to claims 4, 26, and 50 above, and in further view of Ji et al US Patent No. 6,728,886. Ji discloses a distributed virus scanning arrangement.

29. With regards to claims 16, 35, and 52, Gleichauf, as modified above, fails to teach the protocol being HTTP protocol. Ji teaches a data signature being a message in the form of the HTTP protocol (Ji, column 6 lines 23-38). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Ji's method of detecting HTTP with Gleichauf's adaptive security system because it offers the advantage of allowing the monitoring of a popular method of transferring data across the internet thus reducing the likelihood of a security breach (Ji, column 1 line 63 – column 2 line 8).

30. Claims 17 and 53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al US Patent No. 6,301,668, Vaidya US Patent No. 6,279,113, Olden

US Patent No. 6,460,141, and Ji et al US Patent No. 6,728,886, as applied to claim 16 above, and in further view of Farrow "Security Reality Check."

31. With regards to claims 17 and 53, Gleichauf as modified above fails to teach the detecting of a data signature of "cgi-bin/phf." Farrow teaches the detection of the data signature of "cgi-bin/phf" (Farrow, Page 2, "Stealth Attacks" Paragraph 4). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Farrow's method of detecting the data signature of "cgi-bin/phf" because it offers the advantage of helping prevent attacks because the data signature is a valid indication of an attack upon a system (Farrow, Page 2, "Stealth Attacks" Paragraph 4).

32. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al US Patent No. 6,301,668, Vaidya US Patent No. 6,279,113, Olden US Patent No. 6,460,141, Conklin et al US Patent No. 5,991,881, and Krumel US PGPub 2002/0083331, as applied to claim 23 above, and in further view of Zhang et al "Detecting Backdoors."

33. With regards to claim 24, Gleichauf as modified teaches the data signature being FTP (Conklin, column 3 lines 8-14), but fails to teach the response being a raw shell connection. Zhang teaches teach suspicious behavior comprising the transmitting of a root shell prompt to a suspect node (Zhang, Page 12, Section 4.5, Root Backdoor). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Zhang's method of detecting root shell transmissions with Gleichauf as modified because it offers the advantage of preventing an attack from

Art Unit: 2134

gaining unauthorized access to a system by the use of a backdoor (Zhang, Page 1 Section 1.Introduction).

34. Claim 28 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al US Patent No. 6,301,668, Vaidya US Patent No. 6,279,113, Olden US Patent No. 6,460,141, and Conklin et al US Patent No. 5,991,881, as applied to claim 27 above, and in further view of Bernhard et al US Patent No. 6,275,942.

35. With regards to claim 28, Gleichauf as modified above fails to teach the data signature being passwd in a context where filenames are likely to appear. Bernhard teaches the data signature being passwd in a context where filenames are likely to appear (Bernhard, column 13 lines 20-34). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Bernhard's method of checking for passwd because it offers the advantage of helping ensure that the /etc/passwd file remains secure from attacks (Bernhard, column 13 lines 20-34).

36. Claims 33 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al US Patent No. 6,301,668, Vaidya US Patent No. 6,279,113, and Olden US Patent No. 6,460,141, as applied to claims 25-26 above, and in further view of Krumel US PGPub 2002/0083331.

37. With regards to claim 33, Gleichauf as modified above fails to teach the determining if a packet is an unknown command. Krumel teaches the determining if a packet is an unknown command (Krumel, Page 7, Paragraph 0085, unknown packet

Art Unit: 2134

type). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Krumel's method of detecting unknown commands because it offers the advantage of ensuring that no packets that do not fit set security filters are allowed to pass in and out of a network (Krumel, Page 7, Paragraph 0085 and Page 7 Paragraph 0087).

38. With regards to claim 36, Gleichauf, as modified above, fails to teach the protocol being RPC. Krumel teaches the protocol being RPC (Krumel, pages 23-24, paragraph 0191). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Krumel's method of monitoring the RPC protocol because it offers the advantage of allowing the monitoring of communications between gateways and PLD devices (Krumel, pages 23-24, paragraph 0191).

Conclusion

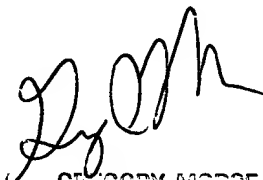
39. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L. Nalven whose telephone number is 571 272 3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 571 272 3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2134

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Nalven



GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100